Dr. Michael Reyer

Tutorial 10

Friday, January 18, 2019

Problem 1. (*Singular points on elliptic curves*) Let $E : Y^2 = X^3 + aX + b$ be a curve over the field K with $\operatorname{char}(K) \neq 2, 3$ and let $f := Y^2 - X^3 - aX - b$.
A point $P = (x, y) \in E$ is called *singular*, if both formal partial derivatives $\partial f/\partial X$ and $\partial f/\partial Y$ are zero at P.

Prove for the discriminant Δ of the curve E that the following holds:

$$\Delta \neq 0 \Leftrightarrow E \text{ has no singular points.}$$

Problem 2. *(Working with elliptic curves I)* Consider the equation

$$Y^2 = X^3 + X + 1.$$

a) Show that this equation describes an elliptic curve E over the field $\mathbb{F}_7$.

b) Determine all points in $E(\mathbb{F}_7)$ and compute the trace t of E.

c) Show that $E(\mathbb{F}_7)$ is cyclic and give a generator.